Before the
Federal Communications Commission
Washington, D. C. 20554

In the matter of	)	
	)	
Review of the Emergency Alert System	)	**EB Docket No. 04-296**
	)	
	)	
	)	
	)	
	)	
	)	

Comments of
Gerald M. LeBow
Harold E. Price
Developers – Sage Alerting Systems ENDEC

I. Introduction

As the developers of the Sage ENDEC and a number of emergency alert and warning systems and technologies, we submit herewith our comments on the Notice of Proposed Rulemaking. The Sage ENDEC was referenced in the FCC Notice page 7 footnote 36. We participated with the Commission in the field tests leading up to the creation of FCC Part 11 which defines the Emergency Alert System. We have also participated in a number of committees and panels including the PPW (Public Private Warning Partnership).

Over the years, we have communicated our concerns about the Emergency Alert System to the Commission and to FEMA. Sage Alerting Systems is on record as having filed comments in 1993 and 1994 under FO Docket No. 91-171 and 91-301 which dealt with

the original definition of the Emergency Alert System. At that time we raised significant concerns about the slow speed FSK technology proposed, the lack of security, the lack of addressability, and the lack of mandatory requirements for EAS participation. We are heartened by the Commission's current Notice of Proposed Rulemaking, 10 years after the original rulemaking, which seeks to improve the EAS.

The comments below represent many years of experience with broadcasters, the Emergency Management Community and the public. We hope these comments are helpful to the Commission in its noble effort to modernize the Emergency Alert System.

II. Discussion.

In paragraph 20 the Notice seeks comment on whether the existing EAS system is the most effective and efficient public warning system.

We believe that public warning systems must be looked at as a 3-prong approach;

1. Capture of data from the initiator
2. Movement of data in the notification network
3. Dissemination to the public.

The current EAS system primarily concerns itself with the 3rd prong, dissemination to the public. The EAS system uses the same method of initiation and movement through the network as it does in the last mile dissemination to the public. As we have stated

numerous times to the Commission, FEMA and other government agencies, we are deeply concerned about security in the first two phases of the EAS process. The current EAS system is extremely vulnerable to sabotage because there is no security and encryption used in the back channel networks. It is easy to replicate EAS tones and inject them maliciously onto RPU (Remote Pick up Unit) frequencies, public safety repeaters and even into studio equipment. Since the EAS system is, for the most part, automated, such spoofing of the system could cause the dissemination of an alert to the public which was not intended. The result could be chaos and panic or at the very least, a loss of confidence in the EAS system.

We also believe, as does PPW and MSRC, that compatibility with the existing EAS/WRSAME standards should be maintained, if possible. That means that consumer receivers such as WRSAME radios should still be supported even if the transmission protocol is changed or modified. This can be accomplished by keeping existing EAS systems operational even if a new protocol is adopted. In addition, the dissemination to the public should be broadened beyond radio, TV and cable channels to include cell phones, satellite TV, digital radio, DARS, HDTV channels, and any medium which can reach the public in their homes, schools, cars or offices.

The new EAS system needs to be much more selective in its reach of the public. The current EAS system offers selectivity down to 1/9 of a county and even that capability is most often not used. The new system needs to be addressable down to an individual home or device so that localized alerts for such things as chemical plant releases,

localized terrorist incidences, flash floods, etc. can be brought quickly and profoundly to those who need it without disrupting the lives of those who are not effected. The more we use EAS, the more the "cry wolf" syndrome will desensitize the public if alerts interrupt them without reason

We believe that there is no one solution to the emergency dissemination problem. A variety of notification methods must be used to reach the largest possible number of the people. EAS, by virtue of the size and expense of the existing installed base should be kept as one of the dissemination methods, however, the first two prongs should be given further attention.

In paragraph 22 the Notice asks whether a single federal entity such as DHS should oversee the national warning system.

We believe that the total responsibility for public alerting and notification through the EAS system must be handled by a single agency which has the responsibility of all three phases of the alerting process as stated previously, i.e., capturing the data, moving the data in the notification network and disseminating it to the public. It would appear that the Department of Homeland Security (DHS) is the natural agency to handle and administer this activity. They should also be given authority to regulate and impose sanctions on broadcasters, cable operators, satellite TV operators, cell phone carriers, etc. who do not conform to the new EAS rules.

In paragraph 24 the Notice raises the question as to whether EAS should be voluntary or mandatory.

Since 1993 in our earliest comments, we have implored the Commission to make EAS activations and participation mandatory, without exception. The notion that a disc jockey, new on the job, at 2 A.M. is going to have to decide whether or not to carry an alert from a chemical plant which has just released toxic gas boggles the mind. Federal, State and Local agencies must be given the authority to activate the EAS system when necessary and media must be mandated to make their facilities available be it a cell tower, FM broadcast station, satellite transponders, etc. to reach the effected people with as much timely information as the emergency management community deems necessary. The current voluntary system leaves the public vulnerable and corrupts the fundamental premise for public warning and notification system.

We realize that the "must carry" rules are extreme and controversial, and to some extent the local community needs (is this Tornado alley, is there a Nuclear power plant in the area, etc) must be taken into account. However, we strongly believe that ALL licensed broadcast entities should at least be required to fulfill the obligations of a State or Local emergency plan. This includes the requirement of updating all equipment to the current level of part 11 including all of the current non-required activation codes. In addition, such licensees should be required to immediately transmit such additional alerts beyond the EAN and EAT, as designated either by the Commission or the State plan.

In paragraph 27 the Notice talks about the PEP program.

We worked with the PEP program and developed unique secure protocols so that equipment at each of the PEP stations could be automatically activated to capture the broadcast channel.

The fallacy of the PEP system was, and continues to be that it is activated through a series of dial up phone lines activated from several locations around the country. We all know that phone lines are subject to outages, congestion, and are certainly not reliable enough on which to base the safety of 300 million U.S. residents.

We believe that a redundant, rugged and reliable backbone network must be created not only between the federal government and the PEP stations, but between all emergency management locations, media outlets, cell phone carriers and the like. We believe that the primary network should be a fiber based system which could take advantage of the thousands of miles of dark fiber that have been run across the county but have never been lit up. Federal funds should be used to activate this fiber and bring its end points to each of the 3,000+ counties in the United States, 34 PEP stations, thousands of Central Offices for wireless carriers and of course federal agency locations for FEMA, DHS, DOD, etc In essence, we need to rebuild a 21st Century NAWAS system.

As a backup, either a terrestrial microwave network and/or a VSAT network should be built in parallel as a self-healing backup to portions of the fiber network which might be disrupted. This backbone network would go a long way towards localizing alert

transmissions, improve security in the movement of the data in the notification network and provide a stable, reliable, dependable national EAS system. Alternatively, the Internet could be used as a backup system providing sufficient care was given to security, the ability to handle denial of service attacks, etc.

In paragraph 28 the Notice asks if new state and local event codes should be mandatory.

As stated before, we believe that the EAS system's efficacy can only be established if media outlets are mandated to carry all types of alerts which are initiated by Federal State and Local government. Of course, safe guards must be taken to insure that these public-warning agencies, at all levels, act responsively and with security to prevent overuse or misuse of the system.

In paragraph 29 the Notice asks whether other services beyond radio, television and cable should be mandated to participate in the EAS system. Further, the Commission asks whether several of the new digital transmission modes such as DTV, IBOC, DARS, etc. should be included.

The only way an emergency alert and warning system can be effective is if it uses multiple communications medium simultaneously to reach the public. No single medium, radio, television, cable, satellite, etc. will reach 100% of the population 100% of the time. For this reason, all available channels including IBOC digital channels,

multiple DTV digital channels, all satellite TV channels, satellite DARS, closed captions, etc. must be incorporated into the new system.

The Commission should not be overly concerned with legacy systems that are in the field including set top boxes and other kinds of receivers and decoders. The Commission should mandate that as of a certain date, all newly manufactured devices must have a localized warning capability in compliance with EAS rules.

We also believe that the cell phone ring down will be an extremely useful localized tool for emergency management to reach people traveling, working and living in specific areas. Wireless carriers should be mandated to provide the activation service and new handsets and other data terminals should be required to contain the appropriate decoding equipment, after some specific date.

In paragraph 30 the Notice specifically looks at IBOC, DAB, and DTV services which transmit more than one channel or more than one data stream on their assigned frequency.

It make no sense to exclude a listener or viewer who is tuned to a digital channel of an IBOC radio station or one of multiple digital TV streams of a HDTV station from receiving alerts both orally and texturally. .

In paragraph 31 the Notice asks whether technology should be deployed to try and reach the public even when their radios or televisions are turned off.

In 1993 and again today, we continue to believe that it is practical to build receivers with an inexpensive chip that continuously monitors for emergency alert information. This chip would turn a receiver (radio or television) "on" from an "off" state and broadcast the emergency alert at any time of the day or night. This is especially important after midnight when the vast majority of people are not listening to radio or watching television. Such a chip needs to be fabricated at a cost of $1 or less so that the implementation within consumer electronics products including radios, TVs. cell phones, etc. will not be cost prohibitive. The chip could either monitor the broadcast frequency band that the device is designed for (an AM receiver 530-1710 kHz, and FM receiver 88.1-107.9 MHz etc.) or it could monitor one of several unique frequencies specifically designed for emergency alert purposes. In 1994, Sage petitioned the Commission to allocate 10 such frequencies 5 in the VHF range and 5 in the UHF range specifically and exclusively for the purpose of emergency alerting. These channels could be used not only to activate "turned off" units but also as a back channel communications link. These channels, of necessity, need to be encrypted and secure to prevent malicious activation via these RF paths.

We also believe that mass media is not the only mechanism that can be used. Public address systems in office buildings, amusement parks, schools, hospitals, sports arenas,

etc. could and should be connected to the Emergency Alert System so messages get to people even in environments where they don't have a radio, television, or cell phone.

In paragraph 32 the Notice asks if multiple alerting devices and medium should be included in the EAS system and should there be a mandate to carry emergency messages.

We believe that every method to reach the public in times of emergency should be deployed on a mandatory basis. Technology such as digital road signs currently used for Amber alerts, the Internet, pagers, and of course all conventional media should be included in the EAS system. Congress should pass legislation mandating participating and defining rules of engagement for activation by local state and federal officials.

In paragraph 35 the Notice asks whether consumer electronics equipment should be capable of being turned on from an off state and geographically addressed.

As stated before, we wholly endorse the idea of incorporating inexpensive IC chips which are capable of performing the turn on function in virtually any consumer electronics device. They should have the capability of localization down to an individual home address, street address, zip code or town. A number of schemes including FIPS code and GPS coordinates can be incorporated to insure the localization of alerts.

In paragraph 41 the Notice seeks guidance as to security and encryption as related to EAS.

In 1993, Sage Alerting Systems in its filing on the original EAS docket proposed a secure and encrypted system. Sage would never publish the algorithms used in its proposed system and in fact, by special arrangement with the Commission, submitted such information in a secure fashion so that only those with a need to know were able to see the proposed Sage protocol. Notwithstanding, the Commission never adopted security in EAS. It published all EAS protocols and formats on its web site While one could argue that no security is perfect, certainly having it is better than not having it at all. Today, one can purchase an EAS encoder device without any identification or demonstrated need. The EAS protocol can easily be replicated on any computer sound card.
We would propose something along the lines of Public Key Encryption on all back channel links (RPUs, STLs the 162 MHz NOAA broadcasts etc) leading to an encoder which is capable of transmitting an EAS alert. This would prevent, for the most part, malicious activation. An EAN filter should be required on all remote inputs.. Denial of service or other attacks on the EAS system could be mitigated through the use of multiple activation paths including fiber, land mobile, VSAT, etc.

In paragraph 42 the Notice asks whether localization of emergency messages on cable and broadcast facilities is better than broad distribution.

As stated previously, we endorse localization as an important component of the Emergency Alert System. Providing information only to those who need it and not creating a "cry wolf" syndrome is important to the continued use and respect of the EAS

system. The activation equipment therefore should be placed to provide the maximum localization.

In paragraph 43 the Notice asks about testing of the EAS system and testing of the PEP system.

Over the years, we have been privy to a great deal of information about weekly, monthly and even regional tests which have failed for a variety of reasons, both as users of EAS systems and as support for thousands of radio, TV, cables, and emergency management systems. We see the same jurisdictions failing to conduct successful end-to-end tests time and time again. The causes vary from operator error to poor equipment installation to ineffective backbone communications and everything in between. We think testing must be reported to the Commission or whoever the designated agency or authority is, so that problems can be worked out before real emergencies occur.

In addition, we strongly recommend a nationwide test of the EAN either every year or every two years. An EAN is unique in the way it is handled in each manufacturers equipment in that there is no particular time limit for which an EAN can run. This can only be tested through an actual transmission via the PEP system to all stations and a report from each of the radio TV and cable facilities to the Commission or designated agency.

In paragraph 45 the Notice asks whether EAS participation should somehow be a function of the size of a broadcast or cable operation and their financial capability.

We see no justification whatsoever for limiting the public's access to emergency communications just because the licensee or operator in their area is a small business. As a part of its fiduciary relationship a licensee enjoys with the Commission, including cable operators, every system must be mandated to participate. Should the EAS costs be prohibitive for small operators, the Commission or whatever agency is chosen to oversee EAS should make grants available, on an as needed basis.

In paragraph 46 the Notice asks about enforcement of the EAS system.

We believe that the only way to insure compliance with a mandated deployment and utilization of the Emergency Alert System is for punitive damages to be levied on those who willfully fail to comply with the rules. We think that increasing the fine to $325,000 will certainly get the attention of general managers of radio TV and cable facilities as well as wireless carriers.

We also believe that any automation that the Commission or whatever agency is selected to oversee EAS can use to check for compliance in real time, would be a major

improvement. By asking the ”rabbit to carry the lettuce”, much information about system failures or operational irregularities is never seen by the FCC. By using its own off air monitoring equipment, the FCC can quickly ascertain compliance with rules and regulations.

Conclusion.

We support and endorse the Commission’s Notice of Proposed Rulemaking on the Emergency Alert System. We believe that fundamentally, a number of things must change including:

1. The addition of security and encryption to all back channels.
2. Mandated (non voluntary) activity and activation by ALL licensed media.
3. Incorporation of multiple telecommunications media including satellite, wireless phones and pagers, broadcast and cable media, etc.
4. Alerts must be localized to a device, street address etc
5. All channels (analog and digital) of media facilities must be incorporated as well as capabilities of reaching the public through pubic address systems, and other warning systems in hotels, hospitals, office buildings and stadiums.
6. Automatic “turn on” capability in car home and portable consumer electronics devices should be mandated to insure that messages are received any time of the day or night.
7. Backward compatibility should exist between the existing EAS equipment already installed and an improved EAS system.

8. A backbone network which is secure, reliable and redundant must be incorporated into the activation part of the network linking Counties, States Federal agencies, broadcasters, cable operators, wireless carriers and the like to insure that the messages get out to the public securely and reliably

9. Enforcement is necessary to insure compliance with the mandatory rules of the Commission or whatever agency oversees the EAS.

10. The Commission should, on its volition, monitor the EAS system to determine compliance.

Respectfully submitted:

Gerald M. LeBow
914 328 5745

Harold E. Price
412 835 1530

1700 N. Highland Rd, Suite 401
Pittsburgh, PA 15241